0x Guard

Smart contracts security assessment

Final report

Tariff: Standard

LiquidNFT

September 2022

0xguard.com

hello@0xguard.com

Contents

Introduction

This report has been prepared for the LiquidNFT team upon their request. This project provides liquidity pools for NFT to receive rewards in the form of reward tokens, as well as a loan of funds.

The code is available at Github wise-foundation/liquidnfts-audit-scope. The code was checked in the 292365d commit.

Name	LiquidNFT
Audit date	2022-09-14 - 2022-09-26
Language	Solidity
Platform	Ethereum

Contracts checked

Name	Address
AccessControl	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/AccessControl.sol
Babylonian	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/Babylonian.sol
IChainLink	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/IChainLink.sol
ILiquidInit	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/ILiquidInit.sol

ILiquidPool	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/ILiquidPool.sol
ILiquidRouter	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/ILiquidRouter.sol
LiquidEvents	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/LiquidEvents.sol
LiquidPool	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/LiquidPool.sol
LiquidRouter	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/LiquidRouter.sol
LiquidTransfer	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/LiquidTransfer.sol
PoolBase	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/PoolBase.sol
PoolFactory	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/PoolFactory.sol

PoolHelper	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/PoolHelper.sol
PoolShareToken	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/PoolShareToken.sol
PoolViews	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/PoolViews.sol
RouterEvents	https://github.com/wise-foundation/liquidnfts-audit-scope/blob/292365db70213dac359065afd6c8b667da4777b6/contracts/RouterEvents.sol

Procedure

We perform our audit according to the following procedure:

Automated analysis

- Scanning the project's smart contracts with several publicly available automated Solidity analysis tools
- Manual verification (reject or confirm) all the issues found by the tools

Manual audit

- Manually analyze smart contracts for security vulnerabilities
- Smart contracts' logic check

Known vulnerabilities checked

Title	Check result
Unencrypted Private Data On-Chain	passed
Code With No Effects	passed
Message call with hardcoded gas amount	passed
Typographical Error	passed
DoS With Block Gas Limit	passed
Presence of unused variables	passed
Incorrect Inheritance Order	passed
Requirement Violation	passed
Weak Sources of Randomness from Chain Attributes	passed
Shadowing State Variables	passed
Incorrect Constructor Name	passed
Block values as a proxy for time	passed
Authorization through tx.origin	passed
DoS with Failed Call	passed
Delegatecall to Untrusted Callee	passed
Use of Deprecated Solidity Functions	passed
Assert Violation	passed
State Variable Default Visibility	passed
Reentrancy	passed
Unprotected SELFDESTRUCT Instruction	passed
Unprotected Ether Withdrawal	passed
Unchecked Call Return Value	passed

Floating Pragma	passed
Outdated Compiler Version	passed
Integer Overflow and Underflow	passed
Function Default Visibility	passed

Classification of issue severity

High severity	High severity issues can cause a significant or full loss of funds, change of contract ownership, major interference with contract logic. Such issues require immediate attention.
Medium severity	Medium severity issues do not pose an immediate risk, but can be detrimental to the client's reputation if exploited. Medium severity issues may lead to a contract failure and can be fixed by modifying the contract state or redeployment. Such issues require attention.
Low severity	Low severity issues do not cause significant destruction to the contract's functionality. Such issues are recommended to be taken into consideration.

Issues

High severity issues

No issues were found

Medium severity issues

No issues were found

Low severity issues

1. Functions lacks validation of input parameters (AccessControl)

Status: Open

The contract functions does not check the input addresses against a null address:

1) `_newMultisig` in `updateMultisig()`

2. Few events (LiquidPool)

Status: Open

Many functions from the contract lack events:

1. `changeFeeDestinationAddress()`
2. `addCollection()`

3. Typos (LiquidPool)

Status: Open

Typos reduce the code's readability.

1) 55L 'IliquidInit.sol' should be replaced with 'ILiquidInit.sol'

2) 791L 'functiojn' should be replaced with 'function'

4. Functions lacks validation of input parameters (LiquidPool)

Status: Open

The contract functions does not check the input addresses against a null address:

1) `_chainLinkFeedAddress` in `initialise()`

2) `_newFeeDestinationAddress` in `changeFeeDestinationAddress()`

5. Typos (LiquidRouter)

Status: Open

Typos reduce the code's readability.

1) 16L 'Oracel' should be replaced with 'Oracle'

6. Constructor lacks validation of input parameters (LiquidRouter)

Status: Open

The contract constructor does not check the addresses `_factoryAddress` and `_chainLinkETH` against a null address.

7. Unused import (PoolBase)

Status: Open

The functionality of the `./IChainLink.sol` import is not used in this contract.

8. Typos (PoolBase)

Status: Open

Typos reduce the code's readability.

1) 109L 'corsresponds' should be replaced with 'corresponds'

2) 155L 'cirection' should be replaced with 'direction'

9. Few events (PoolFactory)

Status: Open

Function from the contract lack events:

1. `updateDefaultPoolTarget()`

10. Typos (PoolFactory)

Status: Open

Typos reduce the code's readability.

1) 71L 'mutlisig' should be replaced with 'multisig'

11. Functions lacks validation of input parameters (PoolFactory)

Status: Open

The contract functions does not check the input addresses against a null address:

1) `_newDefaultTarget` in `updateDefaultPoolTarget()`

12. Typos (PoolHelper)

Status: Open

Typos reduce the code's readability.

1) 244L 'resettets'

2) 757L 'merkel' should be replaced with 'merkle'

13. Typos (PoolViews)

Status: Open

Typos reduce the code's readability.

1) 150L 'facotring' should be replaced with 'factoring'

2) 211L 'facotring' should be replaced with 'factoring'

Conclusion

LiquidNFT AccessControl, Babylonian, IChainLink, ILiquidInit, ILiquidPool, ILiquidRouter, LiquidEvents, LiquidPool, LiquidRouter, LiquidTransfer, PoolBase, PoolFactory, PoolHelper, PoolShareToken, PoolViews, RouterEvents contracts were audited. 13 low severity issues were found.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without 0xGuard prior written consent.

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts 0xGuard to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.
OxGuard retains exclusive publishing rights for the results of this audit on its website and social networks.

0x Guard